REMARKS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application is either anticipated under the provisions of 35 USC § 102 or obvious under the provisions of 35 USC § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

If, however, the Examiner believes that there are any unresolved issues requiring adverse action in any of the claims now pending in the application, the Examiner should telephone Mr. Peter L. Michaelson, Esq. at (732) 530-6671 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Specification and abstract amendments

Various amendments have been made to the specification to correct minor inadvertent grammatical, spelling, punctuation and formal errors that still remained in the specification, and to add two missing section headings.

To facilitate entry of these amendments, the Applicants have enclosed herewith a marked-up copy of their specification showing these changes and a new substitute specification that incorporates all these changes. No new matter has been added to the specification. A replacement Abstract is also submitted.

Status of claims

Rather than re-writing their claims, the Applicants, in light of the number of separate amendments that would have been made to the claims, have simply canceled their existing claims and replaced them with new claims 33-67. The new claims more precisely define the present invention and more closely conform to the dictates of US claim practice than the now canceled claims did.

Further, the new claims contain corresponding substantive limitations from the canceled claims, some of which are now effectively combined. To facilitate ready understanding of these new claims, their correspondence with the canceled claims, in terms of the substantive limitations, is indicated by the following table.

Substantive Limitations --
Prior (canceled) vis-à-vis New claims

Prior Claim(s)	New Claim	Prior Claim(s)	New Claim	Prior Claim(s)	New Claim
1	33	17	46	28	59
2+4	34	18	47	29	60
--	35	19	48	30	61
2+5+6	36	20	49	26	62
8	37	21	50	31	63
9	38	22	51	32	64
10	39	31	52	27	65
11	40	23	53	28	66
12	41	24	54	29	67
13	42	25	55		
14	43	26	56		
15	44	27	57		
16	45	31	58		

Rejections under 35 USC § 102

The Examiner has rejected claims 1 and 2 under the provisions of 35 USC § 102(b) as being anticipated by the teachings of the Wood patent (United States patent 5,003,596 issued to M. C. Wood on March 26, 1991). Inasmuch as both of these claims have been cancelled, this rejection is now moot. However, to expedite prosecution, given that these claims have been replaced by corresponding new independent claims 33 and 34, the rejection will be discussed in the context of those new claims. In that context, this rejection is respectfully traversed.

With respect to prior claim 1, the Examiner believed that the Wood patent identically disclosed each of the elements recited in that claim. The Examiner will soon appreciate that with respect to claim 33, his view is incorrect.

By way of background, the Applicants' present invention is directed to a cryptographic process that offers improved security against cryptanalysis and specifically by significantly increasing the difficulty through which a key or plaintext may be deduced from the ciphertext.

As described in page 2, line 20 et seq and page 10, line 23 et seq of the present specification (all page and line references being made to the substitute specification filed herewith), the latter being in conjunction with FIG. 2, one aspect of the invention involves masking plaintext (input) data by using an auxiliary key.

Here, a supplementary key (K*) is applied as input to a supplementary process P*. The supplementary process then computes a primary key K, and may rely on use of a pre-determined auxiliary key K' or not. The primary key and a plaintext block are then both applied as input to a cryptographic process P. Both the supplementary and cryptographic processes form a combined process Q. By virtue of employing a supplementary process, which is not publicly disclosed, the relationship between auxiliary key K' and primary key K is hidden and not known to outsiders. The supplementary process is an inverse of another, invertible function R ($P^* = R^{-1}$). Hence, the supplementary key can be computed, through function R, from the primary key and the auxiliary key. The primary key is secret. By virtue of adding this additional level of complexity to the entire process Q, hardware-oriented cryptanalysis (so-called "Side Channel Attacks") becomes far more difficult. Such attacks rely on observing the behavior of the cryptographic system based on a power consumption analysis and/or I/O timing analysis and, given that behavior, then deducing the data and/or primary key there from. The increased processing complexity provided by the supplementary process essentially masks the processing of the plaintext data and the primary key from Side Channel Attacks thus rendering it far more difficult for the cryptanalyst to derive either the plaintext and/or the primary key from the hardware behavior of the cryptographic device. Further, using a secret process to derive the primary key from a supplementary key further and significantly heightens security inasmuch as the supplementary process P* is not disclosed to the public. Once the ciphertext is generated, it is then compensated to remove affects of the masking, hence producing the same

effects in the ciphertext as if the auxiliary process were not employed.

The Wood patent indeed relates to cryptography and, more particularly, to a system for protecting stored and transmitted data from cryptanalysis. This patent, recognizing the desirability of one-time pads but also their impracticality in practice, aims as its object to create a cryptographic system in which every unique block of plaintext is uniquely transformed, but which requires a single key to do so. See, e.g., col. 3, lines 30 et seq of this patent.

In particular and as described in col. 3, line 53 et seq, a key table is created from an initial key such that the relationship between the keys in the key table can not be determined even if the system implementation is known. From the key table, four blocks of bytes of additional key based determinants are formed which are called masks. The initial key does not exist in either the key table or a mask table. The system preferably uses the key table in a multiple round encryption process. The order in which the keys are chosen is not predetermined or patterned. The system also selects the other encryption functions, including permutations and substitutions, by the plaintext, current state of the ciphertext and the mask values. As such, every block is encrypted with a different combination of permutations and substitutions.

As shown in Fig. 2 and discussed in col. 6, line 26 et seq, the key table is generated using an initial key and optionally an initializing vector. Then,

once the key table is generated, a mask table is produced from entries in the key table. In essence, and as discussed in col. 9, line 7 et seq, each key in the key table is generated as a result of a variable function performed on the previous key, with the process starting with the initial key and thereafter the particular variable function then determined using information extracted from the installed prior or previously generated key. The variable function can not be readily determined from the newly created key. See also, col. 7, line 24 for a detailed discussion of how the key table is produced.

As indicated in col. 11, line 64 et seq, the values in the mask table are used in encryption and decryption to aid in selecting particular entries within tables to perform transformation (substitution and/or permutation) on the data that is to be encrypted or decrypted. This, in turn, further complicates the determination of the key, by a cryptanalyst, from the resulting data.

Fig. 8, and its accompanying discussion in col. 12, line 55 et seq, depicts, in detail, the encryption process. As shown, encryption of plaintext originally represented by numeral 104 takes place in 10 rounds, which are indexed by the variable R. In the first round R=1, the plaintext 104 is permuted according to an entry in permutation table 108, which entry is selected in response to a value from mask table 110 (see Fig. 9 and the corresponding description in col. 14, lines 11-52). In step 114, a key from key table 116 is added to the permuted plaintext, wherein the choice of the key from the

key table depends on the permuted plaintext and a value from mask table 110 (see Fig. 10 for details). In step 122, a further key addition is performed, wherein the key is selected from key table 110 based on the input data to step 122 and a mask value from mask table 110. Then in step 126, an enclave operation is performed on the data according to an entry in enclave table memory 128 in which the entry was itself selected as a result of a value from mask table 110. Furthermore, two subsequent substitution operations 132 and 140 are performed based on S-Boxes stored in S-Box and S'-Box memory 134, which are selected according to a value from mask table 110. These steps are repeated 10 times to finally obtain ciphertext 146 as an output.

The Examiner apparently takes the position that, with reference to col. 12, lines 4-6 and 31-43, the mask creation process described in the Wood patent equals the auxiliary process taught by the present Applicants. This view is incorrect.

As the Examiner can appreciate, the values fetched from mask table memory 110 are only used to determine which permutation/key/enclave/substitution shall be selected from the corresponding table. These values do not mask data as that operation is performed in the present invention. Those values merely select entries within tables that will perform a given function on data to be encrypted or decrypted. Specifically, those values do not serve the same purpose as the auxiliary values, such as a supplemental or auxiliary key, which the

Applicants use in masking their output data and their primary key.

Furthermore, the Wood patent is absolutely silent on compensating the output data (Y), e.g., ciphertext, for any influence which the auxiliary values might have, through use of an auxiliary process (which the present invention employs), on that data. The mask tables disclosed in the Wood patent simply fail to provide any compensation at all -- that is not their purpose, they are merely used for selecting a function. In fact, nothing in the Wood et al patent provides any compensation -- as taught by the Applicants to assure that, while their output data results from increasingly complex processing which effectively masks the key or the plaintext, the same overall plaintext input and key to the process will produce the same resulting ciphertext, hence ensuring compatibility with certain existing key-based cryptographic processes.

Moreover, the aim of the Wood patent is not to protect a system, in contrast to that which the present Applicants teach, that operates with a known cryptographic process against cryptanalysis by masking the data. Rather, the Wood patent seeks to provide a new type of encryption/decryption system (see col. 3, lines 30-49 of the Wood patent).

Independent claim 33 contains suitable recitations directed to the distinguishing aspects of the present

invention. This claim, with those recitations shown in a bolded typeface, is as follows:

> "A method for cryptographically processing data, comprising the steps of:
> a) feeding, to a cryptographic process (P), values of data (X) and a key (K);
> b) performing the cryptographic process (P) to yield cryptographically processed output data (Y);
> **c) feeding, to the process (P), auxiliary values that mask the data (X) used in the process (P); and**
> **d) compensating, by an auxiliary process, influence of the auxiliary values on the output data (Y).**"
> [emphasis added]

Given that these distinguishing recitations are not shown, taught or disclosed by the Wood patent, then claim 33 is not identically disclosed by the teachings of that patent and hence is not anticipated by those teachings. Consequently, this claim is patentable under the provisions of 35 USC § 102(b).

With respect to prior claim 2, the Examiner believed that the Wood patent identically disclosed each of the elements recited in that claim. The Examiner will soon appreciate that with respect to claim 34, his view is incorrect. Claim 34 contains substantive limitations from prior claims 2 and 4, the latter claim having depended off the former claim and both of which are now canceled.

As discussed immediately above, the Applicants teach the concept of determining their supplementary key (K*) through use of an invertible process (P*).

With respect to claim 4, the Examiner states: "Wood discloses a method wherein the supplementary process (P*) is invertible (8:8-10, 20-22, since you can work backwards to get the original plaintext, the process is invertible)".

In particular, these cited passages expressly state:

> "To decrypt the data, the positioning is rearranged from the bottom to the top to recapture the initial arrangement of the data." (col. 8, lines 8-10) and
>
> "Working backwards through the substitution table, the encrypted data can then be decrypted to recapture the original plaintext values. Once again, this is a standard cryptographic technique and need not be explained in further detail." (col. 8, lines 20-24).

As can be seen, through these passages, the Wood patent merely states that the permutation and the substitution operations performed on the plaintext at steps 106, 132 and 140 are reversible, such that the plaintext can be obtained from the ciphertext. As the patentee readily recognizes, this level of invertability is very well known.

However, merely inverting an encryption process to implement decryption, does not however imply that also the supplementary process (P*), i.e., in the context of the Wood patent being the process of generating a key table from an (original key) and optionally an initializing vector, is or needs to be invertible. Since the Wood patent is silent on using a supplementary process, as the Applicants

specifically teach, this patent contains no teachings pertinent to using such a process that is invertible.

Invertability according to the present application requires that the supplementary key (K*) can he calculated from the inverse of the supplementary process (R^{-1}) given the key (K) and the auxiliary key (K').

The Applicants' distinguishing use of such an invertible supplementary process, as well as other distinguishing limitations as discussed above, is recited in independent clam 34 as follows, with those distinguishing recitations shown in a bolded typeface.

> "A method for cryptographically processing data, comprising the steps of:
> a) feeding, to a cryptographic process (P), values of data (X) and a key (K);
> b) performing the cryptographic process (P) to yield cryptographically processed output data (Y);
> **c) feeding, to an invertible supplementary process (P*), a supplementary key (K*) in order to form the key (K); and**
> **d) wherein:**
> **the supplementary key (K*) masks the key (K) used in the process (P); and**
> **the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed.**" [emphasis added]

Given that these distinguishing recitations are not shown, taught or disclosed, then claim 34 is not identically disclosed by the teachings of the Wood patent and hence is not anticipated by those teachings. Consequently, this claim is also patentable under the provisions of 35 USC § 102(b).

Independent claim 36

Further, independent claim 36, as did prior now canceled claim 6, contains a distinguishing recitation directed to the concept of performing the supplementary process (P*) only when the input data, e.g., plaintext, has certain properties. Though the Examiner did not comment on claim 6 in the prior office action, this distinguishing recitation is also not taught, shown or disclosed by the teachings of the Wood patent. That patent simply has no teachings pertinent to this concept.

This claim, as follows, contains this and other distinguishing recitations, the latter being previously discussed above, with all those distinguishing recitations shown in a bolded typeface.

> "A method for cryptographically processing data, comprising the steps of:
> a) feeding, to a cryptographic process (P), values of data (X) and a key (K);
> b) performing the cryptographic process (P) in order to form cryptographically processed output data (Y);
> **c) feeding, to an supplementary process (P*), a supplementary key (K*) in order to form the key (K);**
> **d) wherein:**
> **the supplementary key (K*) masks the key (K) used in the process (P);**
> **the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed;**
> **the data (X) is also fed to the supplementary process (P*); and**
> **the supplementary process (P*) is performed only if the data (X) has predetermined properties."**
> [emphasis added]

Given that these distinguishing recitations are not shown, taught or disclosed by the teachings of the Wood patent, then claim 36 is also not identically disclosed by the teachings of that patent and hence is not anticipated by those teachings. Consequently, this claim is also patentable under the provisions of 35 USC § 102(b).

Rejections under 35 USC § 103

A. Claims 7, 22 and 27

The Examiner has rejected dependent claims 7, 22 and 27 under the provisions of 35 USC § 103 as being obvious over the teachings in the Wood patent, as applied to claims 1 and 2, and taken in view of the teachings in the Miyano patent (United States patent 5,442,705 issued to H. Miyano on August 15, 1995). Inasmuch as all these dependent claims have now been cancelled, this rejection is also moot. No new claim corresponds to cancelled claim 7. Nevertheless, since new claims 51 and 57 respectively correspond to claims 22 and 27, the rejection will be primarily discussed in the context of those two new dependent claims. In that context, this rejection is traversed. Claims 51 and 57 directly and respectively depend from new independent claims 33 and 34.

The Examiner states that the Miyano patent teaches a method that uses DES. Hence, the Examiner inferentially concludes that one of ordinary skill in the art would modify the cryptographic process taught by the Wood patent to use DES as taught by the Miyano et al patent in order to apparently "increase the security of the system as a whole"

and thus arrive at the Applicants' invention as previously recited in claims 22 and 27.

The Examiner is certainly correct that the Miyano et al patent teaches the use of DES (Data Encryption Standard). DES, in and of itself, is a very well known cryptographic process and, in fact, has been so known since the mid-late 1970s. The Applicants certainly make no claim to the DES algorithm.

As the Applicants discussed in their prior amendment (mailed April 1, 2005), the Miyano et al patent basically relates to a hardware arrangement for transforming plaintext into ciphertext. This patent teaches, as shown in Fig. 1 and discussed in col. 2, line 54 et seq, the use of multiple (n) stages S1-S16 wherein each state encrypts right-hand data R_n by a cipher function F_n in dependence on a key K_n. The results of each cipher function are then combined with left-hand data L_n, through an exclusive OR operation, to form right-hand data R_{n+1} for the next stage, and so forth. The left-hand data L_n produced by each stage becomes right-hand data R_{n+1} for the next stage, and so forth. The initial right- and left-hand data (R_0 and L_0) are the same and are the results of an initial permutation 12. The final right- and left-hand data (L_{16} and R_{16}) are applied to a permutation function 13, which is the inverse of function 12, to form resulting ciphertext.

To provide added security, a different key K_n is used in each stage and renewed at each iteration. Each key is provided by key scheduling section 10 based on an initial key. As discussed in col. 2, line 65 et seq, key scheduling

section 10 is supplied with an initial 64-bit key. This key is transposed by permutation PC-1 shown in Table 1 (in col. 3, lines 6-14 of the patent) which first discards 8 bits of parity and transposes the remaining 56 bits in the order indicated by the table. The resulting transposed bits are split into two halves C and D of 28-bits each. Each half is successively circularly shifted left, by a given number of shifts (as shown in Table 2), to derive each key K_n. Bit data C_n and D_n (n = 1, 2, ..., 16) are then decreased in number from 56 bits to 48 bits via permutation PC-2 shown in Table 3. The resulting 16 keys K_1-K_{16} are respectively applied to stages S1-S16 and stored within corresponding key memories M1-M16 in those stages.

As is the case with the Wood patent, nothing in the Miyano et al patent compensates its output data for any influence which an auxiliary process might have on that data. This patent is simply silent on the use of any compensation, let alone that now taught by the present Applicants; namely, compensation which assures that, while the output data results from increasingly complex processing which effectively masks the key or the plaintext, the same overall plaintext input and key to the process will produce the same resulting ciphertext, hence ensuring compatibility with certain existing key-based cryptographic processes.

Moreover, the Miyano patent also utterly fails to teach the Applicants' use, as discussed above, of an invertible supplementary process (P*) through which a supplementary key (K*) can be generated based on a key (K) and an auxiliary key (K').

Therefore, even if teachings of these patents were to be combined as posed by the Examiner, the resulting combination, would still fall far short of the present invention as recited in independent claims 33 and 34. There are simply no teachings whatsoever in either the Wood or the Miyano et al patents that when combined, would show, disclose or suggest -- whether expressly or even implicitly, the distinguishing features of the invention recited in these two independent claims to a person of ordinary skill in the art, or motivate that person to think in a direction towards those teachings.

Hence, neither of these independent claims is rendered obvious by the teachings of the Wood and Miyano et al patents whether taken singly or in any combination, including that proposed by the Examiner. Therefore, both of these independent claims are patentable under 35 USC § 103.

Dependent claims 51 and 57 respectively and directly depend from independent claims 33 and 34, and recite further distinguishing aspects of the present invention. Consequently, these dependent claims are not rendered obvious by the teachings of these references. Therefore, each of these claims is patentable under 35 USC § 103 for the same exact reasons that its corresponding independent claim is.

B. Claims 21, 23-26 and 28-30

The Examiner has rejected dependent claims 21, 23-26 and 28-30 under the provisions of 35 USC § 103 as being obvious over the teachings in the Wood patent, as

applied to claims 1 and 2, taken in view of those in the Bouricius et al patent (United Sates patent 4,302,810 issued to W. G. Bouricius et al on November 24, 1981). Inasmuch as all these dependent claims have now been cancelled, this rejection is also moot. Nevertheless, since claims 21 and 23-25, and 26 and 28-30 respectively correspond to claims 50 and 53-55, and 56 and 59-61, the rejection will be primarily discussed in the context of these new dependent claims. In that context, this rejection is traversed. Claims 50 and 53-55, and 56 and 59-61 directly depend from or reference (and thus incorporate the limitations of) new independent claims 33 and 34, respectively.

The Examiner cites to the Bouricius et al patent (with the following citations being thereto) for its teachings of:

(a) a method, with respect to claims 21 and 26, "wherein a secure transmission to a host machine of a transaction message describes a financial transaction between a person and a retailer" (col. 3, lines 53-57);

(b) means, with respect to claims 23 and 28, "for an encryption circuit to carryout [sic] an encryption process" (col. 5, lines 37-39);

(c) a method, with respect to claims 24 and 29, "which includes an electronic funds transfer card" (col. 2, line 26); and,

(d) with respect to claims 25 and 30, a portable transaction terminal device (col. 2, line 27).

Hence, the Examiner concludes that one of ordinary skill in the art would modify the cryptographic process, taught by the combination of the Wood and Miyano et al patents, by the

teachings in the Bouricius et al patent to arrive at the Applicants' invention as previously recited in each of claims 21 and 23-25, and 26 and 28-30.

While the Bouricius et al patent does indeed disclose each of the specific elements noted by the Examiner, none of those elements has any bearing on the principal distinguishing aspects of the present invention recited in claims 33 and 34, namely: output data compensation and use of an invertible supplementary process (P*).

Merely adding the teachings of the Bouricius et al patent to the teachings of the Wood and Miyano et al patents would simply result in combined teachings, to the same extent as would arise from combining the teachings in the latter two patents, that would still fall far short of the invention as recited in independent claims 33 and 34. There are simply no teachings whatsoever in the Bouricius et al patent that would provide let alone just suggest the presently inventive teachings which are missing from the Wood and Miyano et al patents to a person of ordinary skill in the art, or motivate that person to think in a direction towards those teachings.

Hence, neither of these independent claims is rendered obvious by the teachings of the Wood, Miyano et al and Bouricius et al patents whether taken singly or in any combination, including that proposed by the Examiner. Therefore, both of these independent claims are patentable under 35 USC § 103.

Claims 50 and 56 respectively directly depend from independent claims 33 and 34, and recite further distinguishing aspects of the present invention. Each of claims 53-55 and 59-61 references and thus incorporates the limitations of new independent claims 33 and 34, respectively. Consequently, all these dependent claims are not rendered obvious by the teachings of these three references. Hence, each of these claims is patentable under 35 USC § 103 for the same exact reasons that its corresponding independent claim is.

C. Claims 31 and 32

Lastly, the Examiner has rejected dependent claims 31 and 32 under the provisions of 35 USC § 103 as being obvious over the teachings in the Wood patent taken in view of those in the Miyano et al patent as applied to claims 22 and 27 and further in view of the Heer et al patent (United States patent 6,028,933 issued to D. N. Heer et al on February 22, 2000). Inasmuch as both of these dependent claims have now been cancelled, this rejection is also moot. Nevertheless, since claims 31 and 32 respectively correspond to claims 52, 58 and 63; and 64, the rejection will be primarily discussed in the context of these new dependent claims. In that context, this rejection is traversed. Claims 52, 58 and 63-64 directly or indirectly depend from new independent claims 33, 34 and 36, respectively.

The Examiner cites to the Heer et al patent for its teachings, expressed in col. 2, lines 62-67, of the use of triple DES in a cryptographic process. Hence, the

Examiner concludes that one of ordinary skill in the art would modify the cryptographic process, taught by the combination of the Wood and Miyano et al patents, by the teachings in the Heer et al patent to arrive at the Applicants' invention as previously recited in each of claims 31 and 32.

The Heer et al patent does indeed disclose using triple DES in a cryptographic system. However, that is irrelevant to the principal distinguishing aspects of the present invention respectively recited in claims 33, 34 and 36, namely: output data compensation, use of an invertible supplementary process (P*), and selectively performing the supplementary process only if the input data, e.g., plaintext, has certain properties.

Merely adding the teachings of the Heer et al patent to the teachings of the Wood and Miyano et al patents would simply result in combined teachings, to the same extent as would arise from combining the teachings in the latter two patents, that would still fall far short of the invention as recited in independent claims 33, 34 and 36. There are simply no teachings whatsoever in the Bouricius et al patent that would provide let alone just suggest the presently inventive teachings which are missing from the Wood and Miyano et al patents to a person of ordinary skill in the art, or motivate that person to think in a direction towards those teachings.

Hence, none of these three independent claims is rendered obvious by the teachings of the Wood, Miyano et al and Heer et al patents whether taken singly or in any

combination, including that proposed by the Examiner. Therefore, all three of these independent claims are patentable under 35 USC § 103.

Claims 52, 58 and 63-64 directly or indirectly depend from new independent claims 33, 34 and 36, respectively. Moreover, each of these claims recites further distinguishing aspects of the present invention. Consequently, these dependent claims are not rendered obvious by the teachings of these three references. Hence, each of those claims is patentable under 35 USC § 103 for the same exact reasons as are its corresponding independent claim is.

Conclusion

Thus, the Applicants submit that none of the claims, presently in the application, is either anticipated under the provisions of 35 USC § 102 or rendered obvious under the provisions of 35 USC § 103.

Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, its swift passage to issue is earnestly solicited.

Respectfully submitted,

October 19, 2005

Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 530-6671

MICHAELSON & ASSOCIATES
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

CERTIFICATE OF MAILING under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited on **October** 20, **2005** with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to the Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Peter L Michaelson — 30,090

Signature — Reg. No.

(PTT111RCEAMEND/ca:159)